Citation
Da Veiga, A., Vorster, R., Li, F., Clarke, N. and Furnell, S.M. (2019), "Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements", *Information and Computer Security*, Vol. 28 No. 3, pp. 399-422.
https://doi.org/10.1108/ICS-11-2018-0135

Comparing the protection and use of online personal information in South Africa and the united kingdom in line with data protection requirements

Adéle Da Veiga and Ruthea Vorster
School of Computing, University of South Africa (Unisa), Johannesburg, South Africa

Fudong Li
University of Portsmouth, Portsmouth, UK

Nathan Clarke
Plymouth University, Plymouth, UK, and

Steven M. Furnell
University of Plymouth, Plymouth, UK

Abstract

Purpose: This research investigates the difference between South Africa (SA) and the United Kingdom (UK) in terms of data protection compliance with the aim to establish if a country that has had data protection in place for a longer period of time has a higher level of compliance with data protection requirements in comparison with a country that is preparing for compliance.

Design/methodology/approach: An insurance industry multi-case study within the online insurance services environment was conducted. Personal Information (PI) of four newly created consumer profiles was deposited to 10 random insurance organisation websites in each country to evaluate a number of data privacy requirements of the Data Protection Act (DPA) and Protection of Personal Information Act (POPIA).

Findings: The results demonstrate that not all the websites honored the selected opt-out preferences as direct marketing material from the insurance organisations in the sample was sent to both the SA and UK consumer profiles. Forty-two unsolicited third party contacts were received by the SA consumer profiles whereas the UK consumer profiles did not receive any third party direct marketing. It was also found that the minimality principle is not always met by both SA and UK organisations.

Research implications: As a jurisdiction with a heavy stance towards privacy implementation and regulation, it was found that the UK is more compliant than SA in terms of implementation of the evaluated data protection requirements included in the scope of this study, however not fully compliant.

Originality/value: Based upon the results obtained from this research, it suggests that the SA insurance organisations should ensure that the non-compliance aspects relating to direct marketing and sharing data with third parties are addressed. SA insurance companies should learn from the manner in which the UK insurance organisations implement these privacy requirements. Furthermore, the UK insurance organisations should focus on improved compliance for direct marking and the minimality principle. The study indicate the positive role that data protection legislation plays in a county like the UK with a more mature stance toward compliance with data protection legislation.

Keywords: POPIA, Protection of Personal Information Act, privacy, DPA, Data Protection Act, GDPR, General Data Protection Regulation, personal information, consumer, direct marketing, opt-in, opt-out, compliance, legal.

1 Introduction

Personal Information (PI) or data is regarded as the new oil in the digital world – a strategic asset, and even a product in itself (*The Economist*, 2017; Sarkhel and Alawadhi, 2017). Since there is an enormous amount of PI collected in cyberspace, organisations are able to gain a competitive advantage through targeted marketing, product customisation (Spiekerman et al., 2015) and the use of value chains (European Commission DG Connect, 2013) to deliver tailored services and products to consumers; nonetheless, the consequences of the utilisation and access to the information of consumers result in consumers experiencing unsolicited marketing emails, invasion of the consumers privacy and fraud (Martin and Murphy, 2017). Studies conducted by Martin (2015) indicated that consumer concerns are reduced if there is increased control by the consumers of their PI and implementation of strong regulatory controls. The importance of regulatory controls has been highlighted by Pelteret and Ophoff (2016, p. 291) as, "Privacy has become a prominent legal issue, with debate about it spurred by constant improvement in technology. With the advent of big data and cloud computing, the legal issues around information privacy have become more complex as data is transported across country boundaries." Research conducted by EMC^2 Corporation in 15 countries found that 87% of respondents agreed that there should be legislation to prohibit organizations from trading consumers data without the 'opt-in' consent (Dell EMC, 2015).

There are over 100 countries with enacted data protection regulations (Greenleaf, 2013). Although these regulations focus on the protection of personal data, the definitions of privacy as well as the conditions for processing and protection vary (Spiekerman et al., 2015). Furthermore, the regulations are enforced more robustly in some jurisdictions, and more moderately in others (DLA Piper, 2018).

The research study reported on in this paper focuses on the data protection jurisdictions of South Africa (SA) and United Kingdom (UK). The South African Protection of Personal Information Act (POPIA) (South Africa, 2013) was signed into law in 2013, and South Africa is regarded as a country in which regulation and enforcement are moderately applied (DLA Piper, 2018). As a consequence, massive data breaches of PI of South Africans were reported during the last five years. The Master Deed's breach of around 60 million SA citizens' identity numbers and addresses were the largest to date. Jigsaw Holdings (a holding company for real estate firms) had stored the information on an unprotected open web server (Fihlani, 2017). In another incident, Liberty Holdings, an insurance organisation, received a ransom request for the company's email repository (Malinga, 2018). In May 2018, the SA Hawks, State Security Agency and the Information Regulator started an investigation of the breach of PI of 943,000 South African drivers. The PI, such as ID numbers and email addresses were stored on the ViewFines website in plain text (Etheridge, 2018). In contrast, the UK Data Protection Act (DPA) (Great Britain, 1998) has been in effect since 2000, and in the UK regulation and enforcement are considered to be robustly applied (DLA Piper, 2018). The Information Commissioner's Office (ICO) in the UK has issued various fines to organisations found to have sold PI for marketing purposes, and to have sent unsolicited text

messages or emails. In recent cases the ICO fined Home Logic UK Ltd (ICO, 2017a) £50,000 for making marketing calls and Moneysupermarket.com (ICO, 2017b) £80,000 for sending marketing emails which recipients did not consent to. In another example, AMS Marketing Ltd was fined £100,000 for making nuisance calls to customers who had opted out for receiving direct marketing calls (ICO 2018b). The maturity and classification of the two approaches differ sufficiently to merit a comparison of practice.

Informed consent is a principle covered by both POPIA and the DPA. Many argue that informed consent is obtained through the opt-out model, in terms of which the user must actively decline or refuse permission for certain processing or use of their PI if they do not want it used in this way. In comparison, the user gives informed consent for certain processing or use of their information within the opt-in model; this is regarded as requiring less effort on the part of the user, and is considered better than the opt-out model in terms of advantage to the user (Noain-Sánchez, 2016). This is made possible using active data collection, whereby an individual knowingly and willingly provides PI on a website (Swire and Berman, 2007). Informed consent also applies when PI is collected online and where organisations plan to use the PI for direct marketing purposes.

For the purpose of this research, informed consent was investigated in the context of obtaining consent for marketing preferences at the time of obtaining online insurance quotes. A case study was conducted in both SA and the UK in which consent for direct marketing, the secure processing of PI, the use of privacy policies on websites, third party sharing of PI, collection of sensitive PI and the principle of minimality in the two countries were compared from a regulatory and compliance perspective in order to make recommendations for improved compliance.

2 Research Objectives

The objective of the research is to compare aspects of data protection compliance between SA and the UK to establish if a country that has had data protection in place for a longer period of time had a higher level of compliance with data protection requirements compared to a country that is preparing for compliance. The results can be used to make recommendations for non-compliance aspects to aid organisations by learning from good practice towards the implementation and regulation of privacy.

The data protection requirements in POPIA and the DPA are similar (Botha et al., 2017; Da Veiga, 2017) and both pieces of legislation incorporate the privacy principles of the Guidelines on the Protection of Personal Information and Trans-border Flow of Personal Data (OECD, 2013) as well as the Fair Information Practice Principles (FIPPS, 2018). As such data privacy implementation in these two countries can be compared. Similar data protection requirements from POPIA and the DPA that could be tested when PI is deposited via a website were selected for the comparison. Consideration was also given to requirements that can be evaluated from a consumer perspective as to whether the consumer will experience that his/her privacy rights, as outlined in the respective regulations, were upheld. As such the following aspects were included for the evaluation: the openness principle whereby consumers must be notified of the purposes and other conditions of processing (typically through an online privacy policy), the secure processing of PI (using Hyper Text Transport Protocol Secure (HTTPS)), the consent for direct marketing (through opt-in for receiving or opting-out to decline) and consent for third party sharing of PI (thereby not receiving unwanted communication from third parties), collection of sensitive PI (not collecting sensitive PI without consent or unnecessarily), and the principle of minimality (not collecting more PI than what is necessary for the purpose).

It is recognised that privacy perceptions differ between consumers (Morton and Sasse, 2014; Kumaraguru and Cranor, 2005). Moreover, cultural aspects also play a role in privacy perception (Greenleaf, 2013; Bygrave, 2010) and even national culture (Da Veiga 2018; Hoffstede et al., 2010). While the aforementioned also play a role in privacy implementation in a country the requirements of the DPA and POPIA were used from a regulatory perspective as the theoretical basis to evaluate the implementation of the privacy requirements in this study. The scope of this research is therefore limited to organisations, being the responsible party, who must implement certain privacy requirements in line with the DPA and POPIA requirements and consumers on the other hand who should through their interaction

with the organisation experience that their privacy rights are maintained in line with the regulatory requirements.

3 Overview of POPIA and the DPA

POPIA and the DPA are both based on the OECD privacy principles (Organisation for Economic Co-Operation and Development, 2013), namely accountability, processing or use limitation, collection limitation, purpose specification, information quality, openness, security safeguards, and data subject participation or access. Both pieces of legislation further include the concept of sensitive PI and cross-border data transfer limitations. POPIA covers breach notification, whereas the DPA does not include it, but the Privacy and Electronic Communications Regulations of 2003 require that organisations notify the ICO in the event of a data breach of personal data (DLA Piper, 2018). Table 1 illustrates the conditions of POPIA that maps to the principles of the DPA (Botha et al., 2017; Da Veiga, 2017). The General Data Protection Regulation (GDPR) mapping is also considered as organisations in the UK might in future also have to comply with its requirements. Table 1 includes a mapping to the OECD privacy principles and FIPPS, indicating that similar privacy principles are covered by both acts allowing for the comparison. The last column indicates which of the principles were selected for inclusion in scope of this study.

Privacy Condition/Principle	FIPPs	OECD	POPIA SA	DPA UK	GDPR	Included in Scope
Accountability	Y	Y	Y	N	Y	N
Processing/use limitation	Y	Y	Y	Y	Y	N
Collection limitation/minimality	Y	Y	Y	Y	Y	Y
Purpose specification	Y	Y	Y	Y	Y	N
Further processing limitation	N	N	Y	Y	Y	N
Information quality	Y	Y	Y	Y	Y	N
Openness	Y	Y	Y	Y	Y	N
Security safeguards and third parties	Y	Y	Y	Y	Y	Y
Data subject participation / access	Y	Y	Y	Y	Y	N
DPO/ IO required	N	N	Y	Y	Y	N
Breach notification	N	N	Y	N	Y	N
Cross-border data transfer limitations	N	N	Y	Y	Y	N
Direct marketing	N	N	Y	Y	Y	Y
Online privacy	N	N	N	N	Y	N
Sensitive PI	N	N	Y	Y	Y	Y

Table 1. Mapping of standards/act requirements to privacy compliance evaluation

The next section provides an overview of the two regulations.

3.1 Overview of POPIA

The PI of SA citizens is protected by the South African Constitution in terms of the common law and the right to privacy as a fundamental human right (South Africa, 1996). POPIA (South Africa, 2013) regulates the processing of PI by public and private organisations domiciled in SA. It defines PI as "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person" (South Africa 2013, p. 14), being the data subject. This includes information such as a person's name, race, language, sex, pregnancy, marital status, and national, ethnic or social origin; information relating to a person's educational level or medical or financial status; the biometric information of a person; the personal opinions or preferences of a person; and even correspondence.

POPIA refers to the organisation that defines the purpose and means of processing of the PI as the "responsible party". There are eight conditions for the processing of PI namely:

- accountability,

- processing limitation,
- purpose specification,
- further processing limitation,
- information quality,
- openness,
- security safeguards and
- data subject participation.

Processing of special PI, rights regarding direct marketing and transborder information flows are addressed as separate chapters in the law. Two conditions are relevant for this research project namely, condition 6 relating to openness, condition 7 relating to security safeguards and the chapter regarding direct marketing requirements. Provisions are also included for the establishment of an Information Regulator. Only the sections relating to the Information Regulator have been enforced to date. The Information Regulator chairperson and members were appointed in December 2016 and have subsequently established the Information Regulator website (Information Regulator South Africa, 2018).

3.2 Overview of the DPA

In the UK, personal data that is stored on computers or in an organised paper filing system is regulated by the Data Protection Act of 1998 (Great Britain, 1998). The DPA regulates the processing and movement of personal data for all purposes other than domestic use. Section 1.1 of the DPA defines personal data as "data which relate to a living individual who can be identified (a) from those data or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller." According to the ICO guidelines entitled "Determining what is personal data", examples of personal data include a person's name, place of work, medical history, and telephone number (ICO, 2012).

The DPA defines how personal data are (or are to be) processed by the data controller. The data controller needs to follow eight principles to ensure that personal data are processed lawfully. Those eight principles are listed in Schedule 1 of the DPA and relate to:

- fair and lawful processing,
- specific and lawful purposes,
- adequate and relevant to the purpose of processing,
- ensuring accuracy,
- not keeping PI for longer than necessary,
- processing in accordance with data subject rights,
- appropriate technical and organisational measures and
- transborder flow requirements.

The rights of data subjects include the right to prevent processing for purposes of direct marketing. This right together with principles 2, 3 and 7 are deemed relevant to this research study. Principle 2 relates to personal data that will not be further processed if the aim of the usage is incompatible with the original purpose of collecting the data (such as further processing relating to direct marketing), principle 3 relates to the minimality principle, and principle 7 establishes appropriate technical measures to be taken against unauthorised processing of the personal data.

4 Overview of Specific Regulatory Requirements

With the aim to compare how organisations in SA and the UK meet the respective privacy requirements, a number of key requirements of POPIA and the DPA were selected, namely direct marketing, openness

using online privacy policies, secure processing and third party sharing. Detailed overviews of these requirements are presented in the next section.

4.1 Overview of Direct Marketing Consent Requirements

POPIA defines direct marketing as communication whereby goods or services are offered to a data subject in person, by mail or via electronic communication (South Africa, 2013). Section 69 of POPIA deals with direct marketing using unsolicited electronic communications. A responsible party may contact a data subject only if consent has been obtained, or if the data subject is an existing consumer and communication relates to similar products or services. New consumers may be contacted only once, with consent (opt-in) being required for continued communication. Consent in POPIA refers to "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information" (South Africa, 2013, p. 12). In terms of POPIA, consent for direct marketing is given through consumers electing to opt in. Until POPIA is enacted, the Consumer Protection Act (CPA) of 2010 (South Africa, 2008) gives consumers the right to restrict unwanted direct marketing by opting out. The Information Regulator published a media statement where they emphasised their constitutional mandate to give effect to the right to privacy under which section 69 should also be interpreted (Information Regulator, 2018).

Similar to the definition given in POPIA, Section 11 of the DPA describes direct marketing as communications of any advertising or marketing material that are sent to a particular individual (Great Britain, 1998, s 11). In its document entitled "Direct Marketing," the ICO (2016) presents a number of direct marketing examples, such as a bank contacting a consumer regarding the administration of their bank account and at the same time also introducing its mortgage products. The same section regulates an individual's right to prevent their PI from being processed for the purposes of direct marketing. The Privacy and Electronic Communications (EC Directive) Regulations (Great Britain) 2003 provide more detailed privacy rules for an individual in relation to electronic communications (e.g. email), as these were designed to complement the DPA in respect of people's privacy rights (Great Britain, 2003). From the data controller's point of view, individuals can be contacted (e.g. via email, telephone or text message) only if they have consented to this (e.g. by means of opt-in or opt-out boxes) (ICO, 2016).

This requirement can be tested by evaluating if websites include an opt-in or opt-out option that consumers can select to indicate their preference in receiving direct marketing. The compliance of the organisation with the consumer preferences can be monitored through the direct marketing communication received on the personal email or cell phone numbers provided by a consumer. Figure 1 shows an example of how websites could include the opt-in option for marketing preferences.

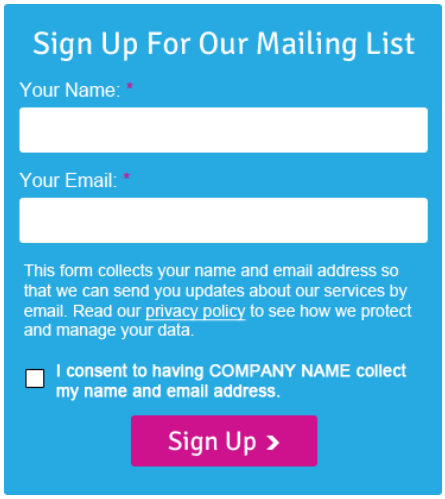


Figure 1: Opt-in for marketing (Siruss, 2018)

4.2 Overview of Openness Using an Online Privacy Policy

Where PI is captured actively on websites, the website should include a link to a privacy policy or notice that is clear and easy to access (Swire and Berman 2007). This privacy policy should explain to the data subject what their PI will be used for and with whom it will be shared, and thus ensure that the data subject is aware of the purpose of information collection and other aspects to meet the requirements of the openness condition/principle.

POPIA requires the responsible party to notify the data subject about a number of aspects by means of a privacy policy or notice disclosing all the means by which the organisation collects, uses and discloses PI (South Africa, 2013, s 18). Principle 1 of DPA Schedule 1 states that "Personal data shall be processed fairly and lawfully". One of the ways to uphold this principle is to provide, in a privacy policy, additional information on how personal information is collected and processed, who the data controller is and the purpose for which the information will be processed (ICO, n.d.).

This requirement can be checked by establishing if websites have a privacy policy or includes privacy notices in their terms and conditions. Figure 2 illustrates a website sign-up form with both non-compliant and compliant examples in terms of agreeing to the terms and conditions and privacy policy (Siruss, 2018).

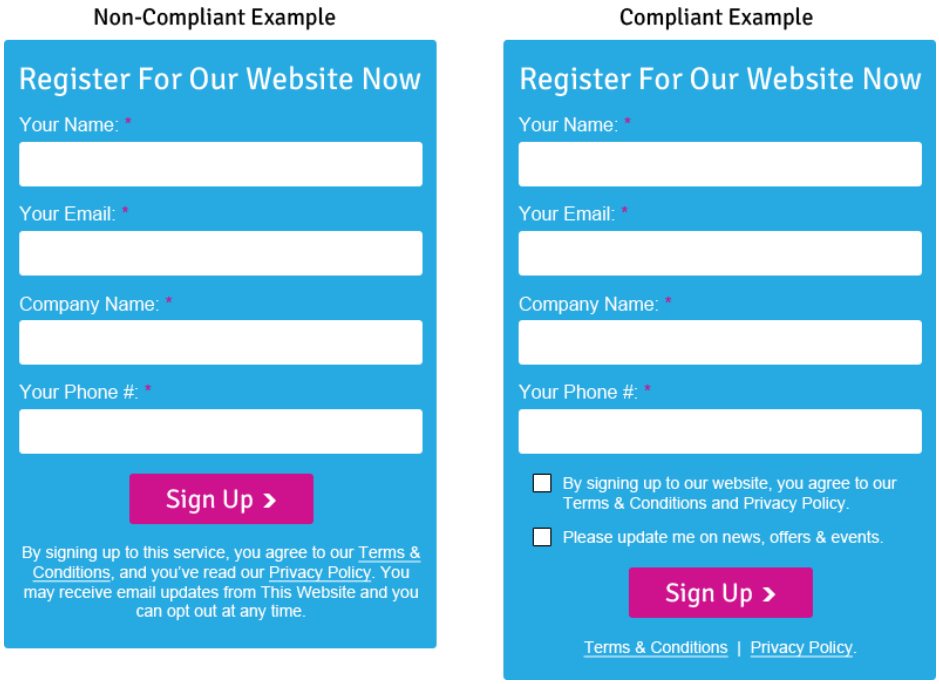


Figure 2: Agreeing to the terms and conditions and privacy policy (Siruss, 2018)

4.3 Overview of Secure Processing Requirements for Websites

Condition 7 of POPIA requires that a responsible party must secure the integrity and confidentiality of PI that it processes by applying technical and organisational measures to protect it (South Africa 2013, s 19(1)). As mentioned earlier, principle 7 of Schedule 1 of the DPA states that proper security controls should be used to protect PI from being misused. More specifically, the ICO document entitled "Protecting personal data online services" provides guidelines on various security mechanisms that can be used to protect PI online, including configuration of Secure Socket Layer, good password usage, and software security updates (ICO, 2014). This will aid in preventing the loss, destruction, unauthorised

access and processing of PI. In addition, it is also the responsibility of the responsible party to inform the data subject if a data breach occurs. For the purpose of this research, the use of HTTPS as one of the various security mechanisms was considered owing to the ease of identifying it for the case study.

The security processing of PI via websites can therefore as a minimum requirement (although not the only) be verified by checking if an organisation's website uses HTTPS when a consumer deposits his/her PI on the websites, especially where sensitive PI is collected.

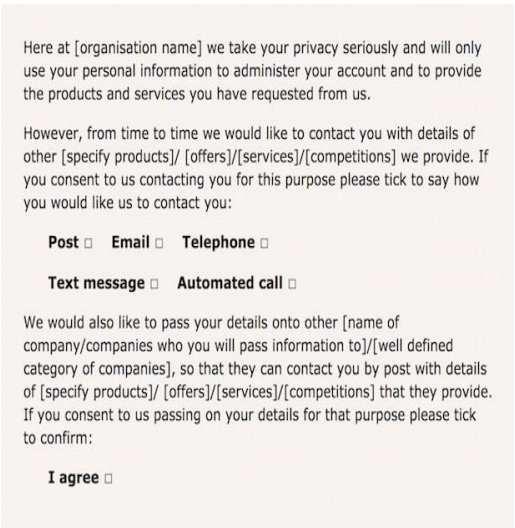
4.4 Overview of Third Party Requirements

Consent for direct marketing does not constitute consent to share or sell PI to third parties for direct marketing. Section 18 of POPIA requires a responsible party to take reasonable practical steps to notify the data subject of the recipient or categories of recipients of their PI. Furthermore, PI may be supplied to third parties only if this serves the legitimate interests of the responsible party or third party (South Africa 2013, s 11(f)). It is important to note that the purpose of collecting the PI must be explicitly stated, and must be lawful (South Africa 2013, s 13(1)). Any sharing of PI with a third party should be communicated to the data subject and must be in line with the original purpose of collection. Where PI is shared with a third party for legitimate reasons there must be a written contract in place between the responsible party and the third party outlining the security requirements to ensure that the integrity and confidentiality of the PI is secured (South Africa 2013, s 20 and s 21). It is the responsibility of the responsible party to ensure that a contract is in place stipulating the security measures and to ensure that the security measures are maintained (South Africa 2013, s 21).

The openness condition of POPIA stipulates that, "If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of—…(h) any further information such as the – (i) recipient or category of recipients of the information" (South Africa 2013, s 18. (h)(i)). A responsible party may not transfer PI to a third party in a foreign country unless certain provisions are in place, such as a binding code of conduct or contract, or unless the data subject consents to this (South Africa 2013, s 69).

Section 70(1) of the DPA defines a third party as any person other than "a) the data subject, b) the data controller or c) any data processor or other person authorised to process data for the data controller or processor". In terms of data sharing, Schedule 3 Section 4 of the DPA states that disclosure of sensitive personal data to third parties can be processed only if the consent of the individual is given. As a result, many data collectors use a privacy notice to explain to individuals how their personal data will be processed (e.g. the sharing of their data with third parties if required) during the data collection phase (Audiencedatasharing, n.d.) and the individuals can then decide whether to give permission to the data collector to allow third parties to use their personal data.

This requirement can be evaluated by establishing if websites notify consumers or obtain consent for sharing the consumer's PI with third parties. In addition, compliance can be verified through the communications which the consumer receives on his/her email or cell phone number as deposited on the website, which should not include third parties that are not related to the purpose of sharing the PI. Figure 3 shows an example of how the opt-in for sharing with third parties can be phrased (itseeze websites, 2018).


Here at [organisation name] we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

Post □ **Email** □ **Telephone** □

Text message □ **Automated call** □

We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:

I agree □

Figure 3: Opt-in for third party sharing (itseeze websites 2018)

4.5 Overview of the Minimality Principle

The minimality principle in both POPIA and the DPA are similar in that it requires responsible parties to ensure that the PI collected must be adequate, relevant and not excessive. The ICO published guidelines on their website explaining adequacy as being, "sufficient to properly fulfil your stated purpose"; relevant, as having, "a rational link to that purpose"; and limited as being, not processing, "more than you need for that purpose." (ICO, 2018b). Online organisations therefore have the responsibility to ensure that the fields of PI collected online is not excessive whilst ensuring that the accuracy of collected PI is maintained as well as the security. For the purpose of this research the fields of PI collected can be evaluated to determine if all fields collected are necessary to fulfil the purpose for obtaining online insurance quotes.

4.6 Overview of Sensitive Personal Information

The definition of sensitive PI in both POPIA and the DPA relates to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject as well as the criminal behaviour or offences. Section 27 of POPIA requires that sensitive PI may only be processed if the data subject provides consent; if it is necessary for a defence of obligation of law; it relates to historical, statistical or research purposes in line with certain provisions that apply. The DPA specifically includes the word "explicit" where consent must be obtained for the processing of PI. Where explicit consent is not obtained one of the other provisions in Schedule 3 of the DPA must apply, such as when the processing is necessary for legal proceedings, if it is in the vital interests of the data subject or another person or for medical purposes.

4.7 Summary of Regulatory Requirements to be Tested

The regulatory requirements that will be tested in the scope of this research study is summarised in Table 2. Column one portrays the relevant condition followed by the regulatory requirements of POPIA and the DPA in columns two and three respectively. A summarised purpose is provided in column four with a description of how the requirement will be tested within the scope of this research.

Condition / principle	Regulatory requirement POPIA	Regulatory requirement DPA	Purpose	Requirement to be tested
Openness principle	**Condition 6: Notification to data subject when collecting personal information** 18. (1) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of— (a) the information being collected and where the information is not collected from the data subject, the source from which it is collected; (b) the name and address of the responsible party; (c) the purpose for which the information is being collected; (d) whether or not the supply of the information by that data subject is voluntary or mandatory; (e) the consequences of failure to provide the information; (f) any particular law authorising or requiring the collection of the information; (g) the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation; (h) any further information such as the— (i) recipient or category of recipients of the information; (ii) nature or category of the information; (iii) existence of the right of access to and the right to rectify the information collected; (iv) existence of the right to object to the processing of personal information as referred to in section 11(3); and (v) right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.	**Part II** **Rights of data subjects and others** **7.**—(1) Subject to the following provisions of this section and to Right of access to sections 8 and 9, an individual is entitled— personal data. (a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller, (b) if that is the case, to be given by the data controller a description of— (i) the personal data of which that individual is the data subject, (ii) the purposes for which they are being or are to be processed, and (iii) the recipients or classes of recipients to whom they are or may be disclosed, (c) to have communicated to him in an intelligible form— (i) the information constituting any personal data of which that individual is the data subject, and (ii) any information available to the data controller as to the source of those data, and (d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.	Consumer notification of purpose and other conditions of privacy	Online privacy policy on website or in terms and conditions
Secure processing requirement of websites	**Condition 7: Security safeguards** 19. (1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent— (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information.	**Principle 7** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	Ensure data integrity and confidentiality	Use of https on website
Direct marketing consent	**Direct marketing by means of unsolicited electronic communications** 69. (1) The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the	11.—(1) An individual is entitled at any time by notice in writing to a processing for data controller to require the data controller at the end of such period as purposes of direct is reasonable in the circumstances to cease, or not to begin, processing for	Consumer provided with the option to choose	Option provided on website to opt-in to receive direct marketing communication

Condition / principle	Regulatory requirement POPIA	Regulatory requirement DPA	Purpose	Requirement to be tested
	data subject— (a) has given his, her or its consent to the processing; or (b) is, subject to subsection (3), a customer of the responsible party. (2) (a) A responsible party may approach a data subject— (i) whose consent is required in terms of subsection (1)(a); and (ii) who has not previously withheld such consent, only once in order to request the consent of that data subject.	marketing. the purposes of direct marketing personal data in respect of which he is the data subject. (2) If the court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit. (3) In this section "direct marketing" means the communication (by whatever means) of any advertising	to receive marketing communication	
Consent for 3rd party sharing	**Condition 4: Further processing** 15. (1) Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13. **Condition 6: Openness** 18. (1) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of— any further information such as the— (i) recipient or category of recipients of the information **Condition 7: Security measures regarding information processed by operator** 21. (1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.	**Principle 2** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. **Schedule 3 Processing of sensitive personal data** The processing— (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.	Notification and consent for third party sharing	Option to consent for 3rd party sharing of PI
Minimality principle	**Condition 2: Minimality** 10. Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.	**Principle 3** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Collecting the minimum fields of PI given the purpose	Review fields of PI collected be in line with purpose and not excessive
Collection of sensitive PI	26. A responsible party may, subject to section 27, not process personal information concerning— (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings. 27. (1) The prohibition on processing personal information, as referred to in section 26, does not apply if the—	"sensitive personal data" means personal data consisting of information as to - data. (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992 c. 52. 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or	Consent for special personal information in line with purpose	Review if special PI collected are in line with purpose

Condition / principle	Regulatory requirement POPIA	Regulatory requirement DPA	Purpose	Requirement to be tested
	(a) processing is carried out with the consent of a data subject referred to in section 26; (b) processing is necessary for the establishment, exercise or defense of a right or obligation in law; (c) processing is necessary to comply with an obligation of international public law; (d) processing is for historical, statistical or research purposes to the extent that	(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.		

Table 2. Summary of regulatory requirements to be tested

5 Research Methodology

A multi-case study methodology with multiple units of analysis was utilised to conduct this research study (Yin, 2003). The multi-case study methodology follows a replication logic through the selection of two countries, SA and UK. More than one unit of analysis are included in each country, namely ten short-term vehicle insurance organisations in each country. The privacy compliance requirement tests, as defined at the beginning of the research study in section four, are replicated across the organisations in each country. Ethical clearance for this research project was obtained through the relevant research ethics bodies at the University of South Africa (Unisa) and the University of Plymouth. Ethical clearance required data anonymisation and confidentiality of the organisations included in the sample, and therefore no organisation names or distinguishing characteristics are disclosed in the research result discussion.

5.1 Case Study Overview

The insurance industry was selected for the research study due to several reasons. Firstly, the insurance industry processes large volumes of personal information (Norton Rose Fulbright, 2013) and are regarded as one of the industries that are affected by a large number of data breaches (PwC, 2015). Also, the insurance industry provides consumers with the service of obtaining online insurance quotes. During this process consumers deposit their PI online which enabled the researchers to conduct the case study to test the selected privacy requirements. The convenience sampling method was used to select the insurance organisations (Etikan et al., 2016).

To facilitate the data depositing and data collection four new cellular phone SIM cards were linked to four newly created email addresses for each country, thus eight user profiles in total. In each country, two of the cellular numbers were used to opt in and the other two cellular numbers were used to opt out for direct marketing in order to monitor compliance with direct marketing preference (see Table 2).

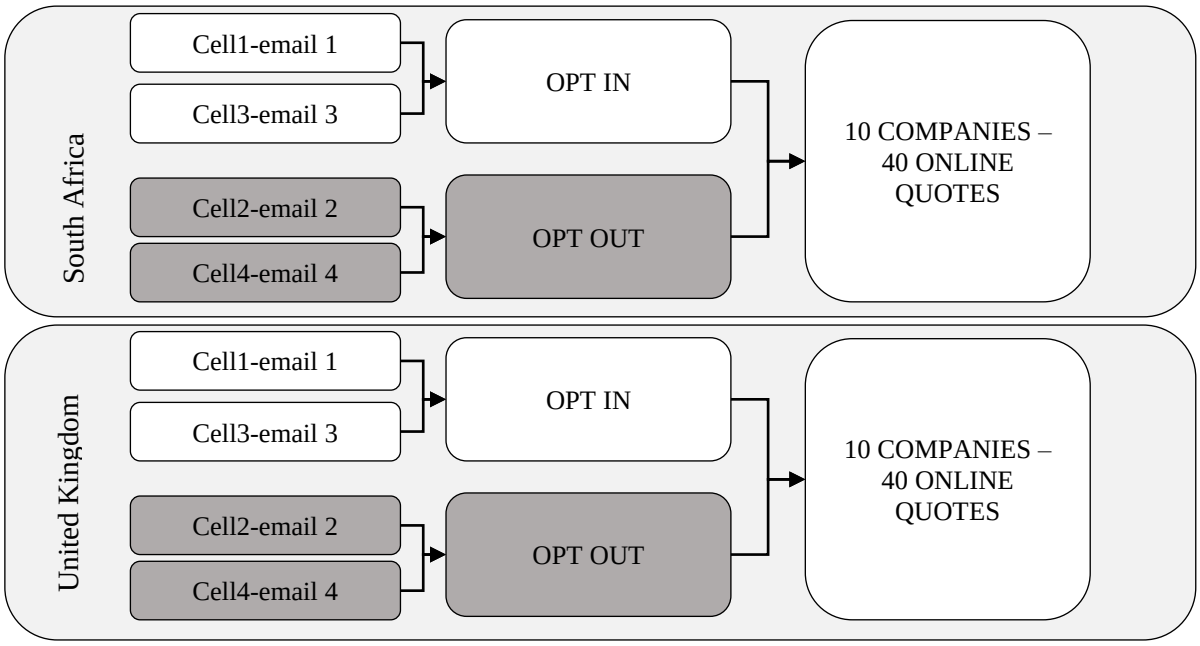


Figure 4. Data depositing plan for the 10 organisations in each country

The researchers requested online quotes for each cell number and corresponding email. Thus, in SA the four SA profiles were used to request quotes at each of the ten insurance organisations with a total of

forty online quotes. Similarly, forty online quotes were obtained in the UK. As such PI was deposited on the websites of the ten insurance organisations included in the sample for each country. The PI requested on the websites, the use of HTTPS on the website and the availability of a privacy policy and/or disclaimer were noted during the depositing process. All cell phone calls, short messages (SMS) and emails received resulting from the request for an insurance quotation were recorded for a period of three months.

In addition to POPIA, the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA) (South Africa, 2003) also plays a role in the collection of PI in SA. RICA requires telecommunication organisations to verify the identity of a consumer through their personal identification documentation and to retain copies thereof. For one of the SA profiles the cell phone provider requested the personal identification documentation, but the second cell phone provider did not adhere to these requirements for verification. The UK cell phone provider did not require any PI when the SIM cards were purchased.

6 Results

All cellular telephone calls received, SMS and emails received were recorded in a MS-Excel spreadsheet, noting the identity of the caller/contact, which organisation contacted the data subject, the nature of the contact, e.g. was it insurance related and if the data subject had opted in or opted out to receive any direct marketing communication from the insurance organisation. The evidence was quantified and analysed firstly per country and thereafter both countries results were compared and evaluated for differences and/or similarities.

6.1 Overview of PI Collected

There was variation in the PI requested of the data subjects by the insurance organisations in the SA sample, whereas the PI requested by the UK insurance organisations was more consistent. Table 3 summarises some of the PI requested to indicate the variation between the two countries.

PI requested	Number of websites		PI requested	Number of websites	
	SA	UK		SA	UK
Name	9	10	Physical address	1	10
Surname	8	10	Marital status	3	10
ID	7	0	Vehicle registration number	1	10
Gender	0	2	Secure parking	3	1
Birth date	0	10	Driving with disability/medical condition	1	2
Cell phone	9	10	Driving record (judgment)	1	10
Email address	7	10	General vehicle details (e.g. model, model, year)	5	10

Table 3. PI requested

In SA, a person's identity number can be utilised to deduce their birth date, age and gender (Western Cape Government, 2016), and this number was validated as part of the online request for authenticity. Where the email address was not requested by the SA websites, the cell number was requested and vice versa. One of the SA websites requested information about disability status. This is classified as "special personal" information by POPIA, as it falls under health information (South Africa 2013, s 26), which may not be processed unless consent is obtained, or certain other provisions apply. Of concern is that this website was also one of the websites that did not include an option for direct marketing preferences.

In comparison, the UK insurance organisations requested a wider, but consistent range of PI. The UK does not have a national identity programme, and therefore none of the UK insurance organisations asked for an identity number. The insurance premium paid by drivers is based on their physical address,

which is why all organisations requested this information. Two insurance organisations requested information on whether the insurer had a medical condition that requires the Driver and Vehicle Licensing Agency (DVLA) to be notified.

6.2 Opt-in/opt-out Preferences for Direct Marketing

During the data depositing phase, the availability of an opt-in or opt-out option for direct marketing was recorded to establish and verify whether responsible parties honoured the data subject's choice during subsequent contacts. In the South African sample, only two organisations gave the data subject the choice of either opting in or opting out when it came to receiving direct marketing communication (see Table 4). In the case of two of the SA organisations, the data subject could not proceed with the online insurance quotation request unless the opt-in option was selected (mandatory opt-in). In the SA context, six organisations did not provide either an opt-in or an opt-out option. By contrast, eight of the UK organisations provided an opt-in or opt-out option from which the data subject was free to choose. The remaining two UK organisations set the opt-in by default, with the data subject being able to ask to change their status to opt-out via email or by completing an online opt-out form.

Options	**SA (10 websites)**	**UK (10 websites)**
Opt in/opt out preference available	2	8
Mandatory opt-in	2	2
Use of opt-out form	0	2
No option	6	0

Table 4. Opt-in/opt-out options: SA versus UK

6.3 Use of Privacy Policy

The availability (or absence) of a privacy policy or terms and conditions was noted during the data depositing process. Where nine UK organisations had a privacy policy on their websites and one UK organisation had a privacy notice in terms and conditions on its website. In comparison, five SA organisations had a privacy policy on their websites and also five organisations had a privacy notice in terms and conditions on their websites.

6.4 Security Processing on Websites Using HTTPS

All the organisations included in the UK sample used HTTPS on their websites to process PI for the purpose of the online quotation requests. However, the website of one SA organisation did not.

6.5 Sharing Of PI with Third Parties

None of the SA or UK websites had a third party sharing option or notification at the point of collection. Only one SA organisation had a notice indicating that information would not be shared; however, no option was available to the participant to opt out of third party sharing.

Table 5 sets out the number of contacts received for the opt-out and opt-in profiles in SA and the UK. Of concern is the number of contacts received from organisations that were not part of the sample. In all, 42 contacts were received that were not part of the sample for two of the profiles in SA (20 in the opt-in and 22 in the opt-out group). This indicates that third parties that were not part of the sample contacted the data subjects for direct marketing. The contacts varied from competitions to win airtime, to offers of funeral cover, to product promotions. In comparison, the UK profiles only received contacts from the sampling insurance organisations, regardless of whether they were opt-in or opt-out.

OPT-IN CONTACTS		SA TOTAL	UK TOTAL
Part of sample	SMS - quote follow-up	2	0
	Calls - quote follow-up	19	1
	Email - quote follow-up	15	8
	Email - promotional	3	12
	Total opt-in part of sample	***39***	***21***
Not part of sample	SMS	18	0
	Calls	0	0
	Email	0	0
	Email – promotional	2	0
	Total opt-in not part of sample	***20***	***0***
Total Opt-In Contacts		**59**	**21**
OPT-OUT CONTACTS		**SA TOTAL**	**UK TOTAL**
Part of sample	SMS - quote follow-up	4	0
	Calls - quote follow-up	16	0
	Email - quote follow-up	7	8
	Email - promotional	6	7
	Total opt-out part of sample	***33***	***15***
Not part of sample	SMS	21	0
	Calls	0	0
	Email	0	0
	Email - promotional	1	0
	Total opt-out not part of sample	***22***	***0***
Total Opt-Out Contacts		**55**	**15**

Table 5. Summary of contacts received

Regarding the opt-in and opt-out preferences, 59 and 55 contacts were received by the opt-in profile and opt-out profile respectively in SA, while 21 and 15 contacts were received by the UK opt-in profile and opt-out profile accordingly. The promotional emails received included retail advertisements as well as those relating to insurance. It is not clear whether these were received as a possible result of email profiling or whether they were related to sharing of the email addresses by the organisations in the sample. The 13 promotional emails (six from SA profiles and seven from UK profiles) received as part of the opt-out profile were a concern, as the data subject elected not to receive direct marketing as part of this profile.

6.6 Minimality Principle

The websites included in the SA sample collected up to 31 fields of PI. Table 6 illustrates the total fields of PI collected per organisation as well as the PI fields that could be deemed as excessive in column 3. It is interesting to note that organisation six collected the most fields of PI and in additional also collected sensitive PI such as health (paraplegic, amputee) and criminal PI. Other fields of PI such as the national identification number, dates of when the consumer received his/her first vehicle licence and the employer might also be unnecessary PI for the purpose a vehicle insurance quote. Fields relating to the consumers' name and surname as well as contact details are relevant to enable the organisation to follow up on the quote. The vehicle information is necessary as well as physical address information which

could affect the amount quoted. However, care should be taken to no collect excessive PI which increases the legal obligations of the organisations to secure the information and protect the confidentiality thereof as well as to keep it updated. In contrast the organisations in the UK collected consistent PI With some fields that could be considered excessive.

Organisations	**Total fields of PI collected**	**Excessive PI collected**	**Excessive**
SA Organisation 1	14	Identification number, type of licence, car description	Yes
SA Organisation 2	8	None	No
SA Organisation 3	5	Identification number	Yes
SA Organisation 4	14	Identification number, date of first license, marital status	Yes
SA Organisation 5	5	Identification number	Yes
SA Organisation 6	31	Identification number, other vehicle information, driving with glasses, driving as amputee, driving as paraplegic, judgement in last five years, declared insolvent, declared bankrupt, under administration, under debt review, with whom car is financed, previous insurance, insurance history, marital status	Yes
SA Organisation 7	2	None	No
SA Organisation 8	20	Identification number, with whom car is financed, vehicle registration number, new or second hand, marital status	Yes
SA Organisation 9	4	Identification number	Yes
SA Organisation 10	1	None	No
UK Organisation 1	19	Marital status, employer	Yes
UK Organisation 2	20	Marital status, employer, gender	Yes
UK Organisation 3	20	Marital status, employer, gender	Yes
UK Organisation 4	19	Marital status, health, employer	Yes
UK Organisation 5	17	Marital status	Yes
UK Organisation 6	18	Marital status	Yes
UK Organisation 7	21	Marital status, employer, declared bankrupt	Yes
UK Organisation 8	20	Marital status, employer,	Yes
UK Organisation 9	22	Marital status, employer, declared bankrupt	Yes
UK Organisation 10	25	Marital status, landline, health, employer, declared bankrupt,	Yes

Table 6. Summary of excessive PI collected

Table 6 illustrates the total fields of PI collected per organisation as well as the PI fields that could be deemed as excessive. The total fields of PI collected by the selected SA organisations are different, ranging from 1 to 31. In addition to the minimal requirement, the organisation that collected 31 fields of PI also gathered sensitive PI such as such as health (paraplegic, amputee) and criminal PI. Amongst those excessive PI categories, PI such as the national identification number, and the employer might also be deemed to be unnecessary for the purpose a vehicle insurance quote. A number of SA organisations only collected a few fields of PI with no SA company asking for gender or employer information. This a good from the minimality principle standpoint of view; nonetheless, the quotes from those organisations may not be as accurate as the ones offered by the organisations required more PI. Little difference is presented by the total pieces of PI collected by the UK organisations, ranging from 17 to

25, with three UK organisation that collected information about bankruptcy which might be excessive. In addition most UK organisations asked about the consumers' marital status and employer.

6.7 Sensitive PI

Only one organisation in the SA sample requested sensitive PI. Organisation six required the consumer to declare whether he/she drives with glasses, drive as an amputee, drive as a paraplegic, had a judgement in the last five years, was declared insolvent, was declared bankrupt or was under administration or under debt review. While the consumer can willingly supply the sensitive PI it increases the risk for the organisation collecting the PI. The responsible organisation must ensure that appropriate security measures are in place when the PI is transferred and stored in order to protect the confidentiality thereof. Additional storage space is required and processes to ensure that the data is kept up to date and protected throughout its life cycle. In the event of a data breach the exposed sensitive information could result in a higher impact of reputational damage for the organisation as well as the consumer. Two of the UK organisations enquired about the consumer's health, which could also increase the risk of protecting the information.

7 Discussions

Table 7 provides a summary of the aspects tested in the multi-case study with the results for SA and the UK, and the related observation and recommendations. In the SA context the opt-out preference and third party sharing are of concern – it would appear that organisations do not yet comply with the POPIA requirements. In the UK, the case study data shows that the data collectors do not share PI with third party organisations; nonetheless, individual preference for the opt-out option is not fully honoured, as those who chose the opt-out option were contacted seven times via email and in addition the minimality principle does not seem to be applied.

Requirement	SA	UK	Observation	Recommendation
Opt-in/opt-out available on website	2	8	The SA websites did not comply with this option, although the CPA requires an opt-out option for direct marketing. Most of the UK websites provided an opt-in/opt-out option.	Opt-in/out preferences for direct marketing should be provided on websites at the point of data collection.
Privacy policy on website or in terms and conditions	10	10	All SA and UK websites had a privacy policy or included privacy in their terms and conditions.	N/A
Secure website using HTTPS	9	10	One of the SA organisations did not have a secure website, whereas all the UK organisations did.	SA organisations should ensure secure processing of PI using for example HTTPS.
Third party sharing (Number of third party contacts received)	42	0	A number of contacts were received from organisations that were not part of the SA sample. It is possible that the insurance organisations or the telecommunication organisations shared the data subject's PI without the data subject's knoweldge or consent. In comparison, the UK profiles did not receive anything that was not from the sampling insurance organisations.	SA organisations should ensure that PI is processed lawfully and implement measures to ensure that it is not shared with unauthorised third parties e.g. policy updates, training and awareness to staff, further processing approval process.

Honouring of opt-out (Uncolicited promotional emails received)	6	7	A few promotional emails were received in the opt-out group of the SA and UK profiles. This might be related to the profiling of the email accounts.	SA and UK Organisations should maintain opt-in and opt-out preferences of consumers and exclude consumers from direct marketig if they opted out.
Minimality principle	7	10	More of the UK organisations in the sample collected excessive PI than the organisations in the SA sample, while one organisation in the SA sample collected excessive and sensitive PI.	SA and UK organisations should review data collection forms and remove requests for excessive PI that is not necessary to achieve the purpose.
Senstive personal information	1	2	One of the SA organisations collected health and criminal PI which are classfied as senstive PI.	SA and UK organisations should not collect sensitive PI and should remove the collection thereof from collection forms where it is not necessary to achieve the purpose.

Table 7. Synopsis of results: SA versus UK

The results of this research study indicate that in a country where there is enacted data privacy legislation with an active regulator, the organisations in the sample were more compliant with data privacy conditions than those in a country with pending data privacy legislation. In the UK, the ICO has become more prominent in terms of issuing enforcement actions (which can include monetary penalties and prosecutions) in relation to breaches of the DPA. Indeed, 2017 saw an increase of over 100% in the number of enforcements, and an almost 50% increase in the value of associated fines; the total value of fines has increased significantly over time, as shown in Table 8.

Year	Number of fines	Total value
2010	2	£160,000
2011	7	£541,100
2012	17	£2,143,000
2013	14	£1,520,000
2014	9	£668,500
2015	18	£2,031,250
2016	21	£2,155,500
2017 (Aug)	44	£3,107,500

Table 8. ICO fines 2010–2017 (Metzger, 2017)

In future, the introduction of new legislation will deliver even greater power to persuade and to prosecute non-compliance. To date, the ICO has issued fines of up to £500,000 for DPA contraventions, although in practice it has not issued any above £400,000. However, the permitted threshold will increase significantly with the introduction of the GDPR in May 2018 (Leyden, 2017). Specifically, the GDPR will permit penalties of up to €20 million or 4% of annual global turnover (whichever is higher). Thus, the incentive to comply, and the price of not doing so, will be even greater.

The research results indicate the insurance organisations in the UK sample were more compliant than their SA counterparts. This can be attributed to the longer time frame that the DPA has been in place, the active Regulator and trend of fines imposed. This supports to the work of the DLA Piper that categorises the UK as a country with a heavy stance towards privacy whereas SA is categorised as low (DLA Piper 2018). The SA insurance industry can leverage the results in this study to improve their opt-in/opt-out provisions on organisation websites and to further improve its processes of data sharing with third

parties to ensure that it complies with the provisions of POPIA by obtaining consent for direct marketing and for third party sharing. The UK can focus on implementing measures to comply with provisions for unsolicited marketing in order to honour opt-in and opt-out preferences, to implement measures to obtain consent prior to sending direct marketing material and to meet the requirements of the minimality principle.

8 Limitations

The sample was limited to 10 insurance organisations in SA and the UK, which could be expanded to a larger sample for future research. Although the insurance industry is categorised under the financial sector, it would be advantageous to expand the research sample to other financial sector organisations. The availability of a website policy or disclaimer was noted; however the analysis of website policy content fell outside the scope of this research. In the SA context, contacts received via the cell phone numbers could be the result of previous ownership of a cell phone number, as in this country cell phone numbers are reassigned.

9 Conclusion

The study aimed to compare the process of handling and processing of PI within the online insurance environment across the UK and SA which have difference in terms of privacy adoption/maturity. Nonetheless, the fundamental of both sets of legislations is similar in terms of privacy requirements. In terms of practice, enforcement of regulation appears to be key while maturity also plays a key role, with UK-based practice being more compliance to legislative requirements. With SA still being at an early stage of implementation of the POPIA, with little degree of enforcement, it is left up to organisations to determine suitable policies with regard to PI while preparing for compliance; unfortunately, some chose to monetise rather than to protect the data as evident obtained from this research study. Despite this is a common trend prior to full adoption and enforcement of appropriate legislation, organisations in SA should leverage the results to identify gaps in compliance with POPIA while learning from UK organisations to define their compliance plans.

Acknowledgements

This research is supported by the Women in Research (WiR) Grant from the University of South Africa.

References

Audiencedatasharing (n.d.), "Data Protection What the Regulations Say", available at: https://www.audiencedatasharing.org/asset/26 (accessed 11 September 2017).

Botha, J., Grobler, M. M., Hahn, J. and Eloff, M. (2017), "A High-Level Comparison Between the South African Protection of Personal Information Act and International Data Protection Laws," in *12th International Conference on Cyber Warfare and Security Conference Proceedings (ICCWS) in Dayton, Ohio, USA, 2 -3 March 2017,* Academic Conferences and Publishing International Limited. Reading, UK, p. 57.

Bygrave, L. (2010), "Privacy and data protection in an international perspective", *Stockholm Institute for Scandinavian Law*, Vol. 56, p.165, available at: *https://www.uio.no/*studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf (accessed 20 November 2018).

Da Veiga, A. (2018), "An information privacy culture instrument to measure consumer privacy expectations and confidence", *Information & Computer Security*, Vol. 26 Issue: 3, pp.338-364, https://doi.org/10.1108/ICS-03-2018-0036 (accessed 23 November 2018).

Da Veiga, A. (2017), "The influence of data protection regulation on the information security culture on an organisation – a case study comparing legislation and offices across jurisdictions", In Furnell, S. and Clarke N. (eds.), Proceedings of the *Eleventh International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2017), Australia, Adelaide, pp. 65-79, ISBN: 978-1-84102-428-8.

Dell EMC (2015), "The EMC Privacy Index, Global and In-Depth Country Results", EMC, available at: https://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf (accessed 30 October 2017).

DLA Piper (2018), *"Data Protection Laws of the World, Full Handbook"*, (April 2018), p. 1–513, available at: https://www.dlapiperdataprotection.com/index.html (accessed 17 April 2018).

Etheridge, J. (2018), "Hawks, SSA probing major 'leak' of personal data of SA drivers who use ViewFines", *News24,* available at: https://www.news24.com/SouthAfrica/News/hawks-ssa-probing-major-leak-of-personal-data-of-sa-drivers-who-use-viewfines-20180524 (accessed 22 August 2018).

Etikan, I., Musa, S.A. and Alkassim, R.S. (2016), "Comparison of Convenience Sampling and Purposive Sampling", *American Journal of Theoretical and Applied Statistics* Vol. 5 Issue: 1, pp. 1–4, available at: 10.11648/j.ajtas.20160501.11 (accessed 15 October 2017).

European Commission DG Connect (2013), "A European strategy on the data value chain", available at: https://ec.europa.eu/digital-single-market/news/elements-data-value-chain-strategy (accessed 15 October 2017).

Fair Information Practice Principles (FIPP) (2018), "IT Law Wikia", available at: http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles (accessed 29 March 2018).

Fihlani, P. (2017), "Millions caught in South Africa's worst data breach", *BBC News*, available at: http://www.bbc.com/news/world-africa-41696703 (accessed 28 April 2018).

Great Britain (2003), The Privacy and Electronic Communications (EC Directive) Regulations (PECR), London: The Stationary Office.

Great Britain (1998), Data Protection Act (DPA), London: The Stationery Office.

Greenleaf, G. (2013), "Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories", *UNSW Law Research Paper No. 2013,* Vol. 40 Issue: 29, available at: 10.2139/ssrn.2280877 (accessed 15 October 2017).

Hofstede, G., Hofstede, G. J. and Minkov, M. (2010), *Cultures and Organizations: Software of the mind*, Third edition, The McGraw-Hill Companies, United States, ISBN: 978-0-07-166418-9.

ICO (2018a), "Principle (c): Data minimisation", available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ (accessed 22 August 2018).

ICO (2018b), AMS Marketing Ltd", available at: https://ico.org.uk/action-weve-taken/enforcement/ams-marketing-ltd/ (accessed 20 August 2018).

ICO (2017a), "Home Logic UK Ltd: Monetary Penalties", available at: https://ico.org.uk/action-weve-taken/enforcement/home-logic-uk-ltd/ (accessed 22 October 2017).

ICO (2017b). "Moneysupermarket.com Ltd: Monetary Penalties", available at: https://ico.org.uk/action-weve-taken/enforcement/moneysupermarketcom-ltd/ (accessed 22 September 2017).

ICO (2016), "Direct Marketing", available at: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf (accessed 7 November 2017).

Information Regulator (South Africa) (2017), "Department of Justice and Constitutional Development", available at: http://www.justice.gov.za/inforeg/index.html (accessed 15 August 2017).

ICO (2014), "Protecting personal data in online services: learning from the mistakes of others", available at: https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf (accessed 5 November 2017).

ICO (2012), "Determining what is Personal Data", available at: https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf (accessed 5 November 2017).

ICO (n.d.), "Privacy notices, transparency and control", available at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/ (accessed 7 November 2017).

Information Regulator (2018), "Media statement – Direct Marketing Association of South Africa", available at: http://www.justice.gov.za/inforeg/docs/ms-20180727-DMASA.pdf (accessed 20 August 2018).

Itseeze (2018), "GDPR 101 how to make sure your website is ready for the general data protection regulation", available at: https://itseeze.com/blog/gdpr-101-how-to-make-sure-your-website-is-ready-for-the-general-data-protection-regulation/ (accessed 19 November 2018).

Kumaraguru, P. and Cranor, L.F. (2005), "Privacy indexes: a survey of Westin's studies", Carnegie Mellon University, School of Computer Science, Institute for Software Research International, pp. 368-394, *available as ISRI Technical Report CMU-ISRI-05-138.*

Leyden, J. (2017), "Last year's ICO fines would be 79 times higher under GDPR", *The Register*, available at: https://www.theregister.co.uk/2017/04/28/ico_fines_post_gdpr_analysis/ (accessed 17 November 2017).

Malinga, S. (2018), "Information Regulator is hard at work", *ITWeb*, available at: https://www.itweb.co.za/content/KWEBb7yax8D7mRjO (accessed 14 November 2018).

Martin, D.M. and Murphy, P.E. (2017), "The role of data privacy in marketing", *Journal of the Academy of Marketing Science*, Vol. 45, pp.135-155.

Martin, K. (2015), "Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online", *Journal of Public Policy & Marketing*., Vol. 34, pp. 210–227.

Metzger, M. (2017), "Sharp rise in ICO fines and enforcement notices as GDPR races closer", SC Media UK, available at: https://www.scmagazineuk.com/sharp-rise-in-ico-fines-and-enforcement-notices-as-gdpr-races-closer/article/665466/ (accessed 17 November 2017).

Morton, A. and Sasse, M.A. (2014), "Desperately seeking assurances: Segmenting users by their information-seeking preferences", in *Privacy, Security and Trust (PST), Proceedings of 2014 Twelfth Annual International Conference on Privacy, Security and Trust, 23 – 24 July 2014, in Toronto, ON, Canada,* IEEE, pp. 102-111, ISBN: 978-1-4799-3503-1.

Noain-Sánchez, A. (2016), 'Privacy by default' and active 'informed consent' by layers", *Journal of Information, Communication and Ethics in Society*, Vol. 14 Issue: 2, p. 124–138, available at: 10.1108/JICES-10-2014-0040 (accessed 22 September 2017).

Norton Rose Fulbright (2013), "PoPI and Insurance", available at: http://www.nortonrosefulbright.com/knowledge/publications/74156/popi-and-insurance (accessed 20 November 2018).

Organisation for Economic Co-Operation and Development (OECD) (2013), "The OECD Privacy Framework", available at: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed 29 March 2018).

Pelteret, M. & Ophoff, J. (2016), "A review of information privacy and its importance to consumers and organizations", *Informing Science: The International Journal of an Emerging Transdiscipline*, Vol. 19, pp. 277-301.

PricewaterhouseCoopers (PwC) (2015), "Turnaround and transformation in cybersecurity", available at: https://www.pwc.com/gx/en/ consultingservices/information-security-survey/assets/pwcgsiss-2016-financial-services.pdf (accessed 19 November 2018).

Sarkhel, A. and Alawadhi, N. (2017), "How your personal data sells cheaper than chewing gum", ETtech, available at: http://tech.economictimes.indiatimes.com/news/internet/how-your-personal-data-sells-cheaper-than-chewing-gum/57380518 (accessed 22 September 2017).

Sirrus (2018), "GDPR compliance for websites in 2018", available at: https://www.siruss.co.uk/blog/gdpr (accessed 19 November 2018).

South Africa (2013), Protection of Personal Information Act (POPIA) No. 4 of 2013, *Government Gazette*, Cape Town.

South Africa (2008), The Consumer Protection Act (CPA) No. 68 of 2008, *Government Gazette*, Cape Town.

South Africa (2003), Regulation of Interception of Communication and Provision of Communication-related Information Act No. 70 of 2002, *Government Gazette*. Cape Town, 451(24286).

South Africa (1996), Constitution of the Republic of South Africa Act No. 108 of 1996, *Government Gazette* (No. 17678).

Spiekerman, S., Böhme, R., Acquisti, A. and Hui, K.L., (2015), "The challenges of personal data markets and privacy", *Electronic Markets*, Vol. 25 Issue: 2, p. 161–167, available at: 10.1007/s12525-015-0191-0 (accessed 22 September 2017).

Swire, P. P. and Berman, S. (2007), *Information Privacy, Official Reference for the Certified Information Privacy Professional, e*dited by Kosmala, P., IAPP, Portsmouth, USA, ISBN: 978-0979590108.

The Economist (2017), "The world's most valuable resource is no longer oil, but data", The Economist Group Limited, available at: https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (accessed 22 September 2017).

Western Cape Government (2016), "Decoding your South African ID Number", available at: https://www.westerncape.gov.za/general-publication/decoding-your-south-african-id-number-0 (accessed 19 September 2017).

Yin, R. (2003), *Case study research and applications: Design and methods*, 3rd edition, Sage Publications, California, USA, ISBN: 0-7619-2553-8.